## REMARKS

This is in response to the Office Action mailed on January 11, 2007. Claims 1-48 were pending in the application, and the Examiner rejected all claims. With the present response, claim 3 is amended, and the remaining claims are unchanged. Reconsideration and allowance of all pending claims are respectfully solicited in light of the following comments.

### Claim Objections

On page 2 of the Office Action, the Examiner objected to claim 3 because of informalities. The Examiner stated that "computingdevice" needs a space between the words. Claim 3 has been amended to correct the typographical error.

### Claim Rejections - 35 U.S.C. § 103

On page 2 of the Office Action, the Examiner rejected claims 1-48 under 35 U.S.C 103(a) as being unpatentable over Gould et al. U.S. Pat. No. 6,920,561 (hereinafter "Gould") in view of Michener et al. U.S. Pat. No. 7,028,191 (hereinafter "Michener"). Applicant respectfully contends that the independent claims 1, 23, 27, and 35 are patentable over the cited references considered individually or in combination. Applicant also respectfully contends that at least dependent claims 2-3, 5, 10, 14, 26, 29, 36-37, 39, 43, and 45, are patentable based on the merits of their own limitations.

Claim 1:

On page 3 of the Office Action, the Examiner states that several elements of claim 1 are disclosed by Gould, and that the elements not disclosed by Gould are obvious in view of Michener. Applicant respectfully contends that Gould does not teach or suggest all of the claim 1 elements that the Examiner states that it does, and that at least because of this, claim 1 is patentable.

First, the Examiner states that Gould (figure 4: 414-418) discloses generating a session packet, encrypting it, and transmitting it to the biometric device. As is shown in Gould figure 5, the Gould system consists of a biometric device (292), a client (104), and a server (100). The section cited by the Examiner (figure 4: 414-418) describes the server (100) sending data to the client (104). The section does not disclose transmitting a session packet, or anything else, to the biometric device (292) as is recited in claim 1.

Second, the Examiner states that Gould (figure 4: 420-426) discloses receiving a biometric information packet, decrypting it, and making a determination, based on a content of a collection of information contained in the decrypted biometric information packet, as to whether or not to utilize a collection of biometric data contained in the decrypted biometric information packet. The process described in Gould figure 4: 420-426 first makes a determination of whether or not to utilize the data (Gould figure 4: 420) before it decrypts the data (Gould figure 4: 422). This is a different process than that of claim 1, which very generally speaking, decrypts the data and then makes a determination as to whether or not to utilize the data.

Claim 2:

On page 4 of the Office Action, the Examiner states that Michener (column 9: lines 5-40; Session-Random Number) discloses a method, wherein generating a session packet comprises generating a session number and storing it in the session packet. Applicant respectfully contends that Michener does not disclose this.

The cited section describes using the session random number to generate session keys and re-keying keys. The section does not disclose storing the session random number or any other number, in a session packet.

Claim 3:

On page 4 of the Office Action, the Examiner states that Michener (Column 10: lines 1-25; figure 13: Table Lookup: data structure) discloses a method, further comprising storing the session number in a database associated with the computing device. Applicant respectfully contends that Michener does not disclose this.

Michener figure 13 shows that the "Table Lookup" provides the "TADID_B" value. Michener column 8 line 26, states that this value is a TAD-specific 64 bit Binary ID. This number is not associated with a session, such as the session number recited in claim 3.

Claim 5:

On page 4 of the Office Action, the Examiner states that Michener (column 10: lines 1-15; figure 13: Table Lookup; data structure) discloses storing a session key in a database associated with the computer. Applicant respectfully contends that Michener does not disclose this.

The "Table Lookup" in Michener figure 13 provides the "TADID_B" value which is used to generate a session key. The session key itself is not stored in the "Table Lookup" or in any database associated with the computer.

Claim 10:

On page 5 of the Office Action, the Examiner states that Michener (figure 13) discloses a method, wherein generating a session packet comprises generating a session time stamp and storing it in the session packet. Applicant respectfully contends that Michener does not disclose this.

Michener figure 13 does not contain anything at all related to time. It certainly does not disclose generating or storing a session time stamp.

Claim 14:

On page 6 of the Office Action, the Examiner states that Michener (column 2: lines 15-60; figure 17) discloses a method wherein making a determination comprises evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period. Applicant respectfully contends that Michener does not disclose this.

The text of Michener column 2: lines 15-60 is listed immediately below.

> "various processing stages;
> FIG. 26a illustrates a structure of a TAD input command for loading a rekeying keyset;
> FIG. 26b illustrates a structure of a TAD response to a command for loading a rekeying keyset;
> FIG. 27a illustrates a structure of a TAD input command for installing a new working keyset;
> FIG. 27b illustrates a structure of a TAD response to a command for installing a new working keyset;
> FIG. 28a illustrates a structure of a TAD input command for installing a new language;
> FIG. 28b illustrates a structure of a TAD response to a command for installing a new language;
> FIG. 29a illustrates a structure of a TAD input command for identifying a TAD to a client computer;
> FIG. 29b illustrates a structure of a TAD response to a command for identifying a TAD to a client computer;
> FIG. 30a illustrates a structure of a TAD input command for testing a TAD maintenance key;
> FIG. 30b illustrates a structure of a TAD response to a command for testing a TAD maintenance key;
> FIG. 31a illustrates a structure of a TAD input command for personalizing a TAD; and
> FIG. 31b illustrates a structure of a TAD response to a personalizing a TAD.
> DESCRIPTION OF EMBODIMENT(S)
> Electronic communications, and the data which traverses those communications, are relatively new, as is the technology used to protect electronic data. Existing communications protection technologies tend to fall into two categories. The first, government sponsored, is generally very well thought out and provides excellent protection, but is not readily available for commercial applications. The second, de facto commercial, are mostly not strong enough to protect important information, or are dedicated to specific functions. For example, standard point-of-sale devices are

> dedicated to merchandizing applications, and existing ATM systems are dedicated to the dispensing of cash.
> There exists a need for a device to provide personal protection of electronic data that is small, easy to use, provides excellent protection to the PC/laptop user, and that can operate in conjunction with corresponding devices at a central data gathering point to provide near real time validation of the information."

Applicant fails to see how Michener column 2: lines 15-60 (the language quoted above) could be viewed as disclosing evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period.

Similarly, applicant also fails to see how Michener figure 17 could possibly disclose claim 14. Michener figure 17 does not contain anything similar or related to evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period.

Claim 16:

On page 7 of the Office Action, the Examiner states that Michener (figure 17; column 9: lines 5-35; column 5: lines 20-40) discloses claim 16.

Claim 16 comprises evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period.

The text of Michener column 9: lines 5-35 is listed immediately below.

> "functions:
> 1. Check to make sure that the block is the right length (if wrong, return a failure code and clear the block);
> 2. Calculate the session keys, using the random number Rk provided in the clear text portion, as follows:
> a. Take the first 8 bytes of the session_random number, R1_and calculate session key 1,
> Ks1=EKm1(DKm2(EKm3(R1)))
> (wherein E and D respectively represent the encryption and decryption sub-processes of a symmetric encryption process, e.g. triple DES (3 DES);
> b. Take the second 8 bytes of the session_random number, R2_and calculate session key 2,
> Ks2=EKm3(DKm2(EKm1(R2))); and
> c. Take the third 8 bytes of the session random number, R3 and calculate session key 3,

> Ks3=EKm2(DKm1(EKm3(R3)));
> 3. Decrypt the encrypted portion DKs3(Es2(DKs1(encrypted portion))) using CBC mode;
> 4. Calculate the MD5 hash of the entire block cleartext+decrypted portion (digest block set to NULL);
> 5. Compare calculated digest with received digest (if wrong, return a failure code and clear the block);
> 6. Take the first 8 bytes of the re-keying random number, RKR1 and calculate re-keying key 1,
> KrK1=EKm1(DKm2(EKm3(RkR1)));
> 7. Take the second 8 bytes of the re-keying random number, RkR2 and calculate re-keying key 2,
> KrK2=Ekm3(DKm2(EKm1(RkR2))); and."

The text of Michener column 5: lines 20-40 is listed immediately below.

> "played first information, the captured card information, and all other necessary information (e.g. PIN, location from an associated trusted location device e.g. GPS receiver, etc) as second information in an associated data fields of an associated data structure 42, e.g. illustrated in FIG. 3, wherein the second information is responsive to, or a function of the first information, and may comprise a copy of the first information. Otherwise, from step (206), the process repeats with step (202), wherein the TAD 10 awaits further input from the client 12. Then, in step (208), a random number generator 44—e.g. within the trusted control processor 16—generates a random number R, which may be either a pseudo-random number, or a true random number, for example, generated responsive to a noisy physical process. The TAD 10 may also access and increment a transaction counter, although this step is not essential. Then, in step (210), the trusted control processor 16 generates second information that is responsive to the first information displayed to the user, and which further incorporates the random number R and a first identification code of the TAD 10, e.g. the alphanumeric ID (TADID_A). Then, in step"

Applicant fails to see anything similar to the claim language in the cited sections of Michener, or anywhere else in Michener. Applicant respectfully contends that Michener does not disclose claim 16.

<u>Claim 23:</u>

On page 9 of the Office Action, the Examiner states that Gould discloses a data packet for transmission **<u>from a computer to a biometric device</u>** during a process of authentication within a biometric security system (emphasis added). Applicant respectfully contends that Gould does not disclose this.

Gould figure 5 shows that the Gould system consists of a biometric capture device (292), a client (104), and a server (100). As shown in Gould figure 4: 402-412, data in the Gould system travels from the biometric capture device, to the client, and then to the server. Gould does not disclose any data being sent from the computer (104) to the biometric capture device (292), as is recited in claim 23.

Claim 26:

On page 10 of the Office Action, the Examiner states that Michener (figure 8: 802-808) discloses a method, wherein the session number is a value that corresponds to a session initiated when the data packet is generated.

Michener figure 8: 802-808 consists of the following phrases: "Initiate Transaction On Client Computer"; "Communicate 1st Information to be Authorized to TAD"; "Receive Data Structure from TAD"; and "Communicate Data Structure to Host Computer."

Applicant respectfully contends that Michener figure 8:802-808 (i.e. the quoted phrases above) clearly does not disclose a method, wherein the session number is a value that corresponds to a session initiated when the data packet is generated.

Claim 27:

On page 10 of the Office Action, the Examiner rejects claim 27 as being obvious by Gould in view of Michener.

In rejecting the biometric device of claim 27, the Examiner is using elements not only from the biometric device disclosed in Gould (Gould figure 5 "292"), but also from the client (Gould figure 5 "104") and the server (Gould figure 5 "100"). For example, the Examiner states that Gould figure 3: 308 discloses a biometric receiver. This is referring to the Gould biometric device (292). The

Examiner then states that Gould figure 2: 206 discloses a memory accessibly connected to the processor. This is referring to the Gould client (104).

The Examiner has not indicated why one would be motivated to combine all of these elements into one device. Applicant respectfully submits that it would not be obvious to combine the elements of claim 27 into one device. Evidence of this is shown by Gould itself which discloses a biometric device without all of the limitations of claim 27.

Claim 29:

On page 11 of the Office Action, the Examiner states that Gould (column 3: 25-30) discloses a biometric device wherein the encryption component is implemented in association with a flash memory application. Applicant respectfully contends that Gould does not disclose this.

Gould column 3: 25-30 discloses a flash memory application associated with a PCI-ISA interface. It does not disclose an encryption component implemented in association with a flash memory application.

Claim 35:

On page 13 of the Office Action, the Examiner cites several sections of Gould as disclosing elements of claim 35. Applicant respectfully contends that at least two of the elements are clearly not disclosed by Gould.

First, the Examiner states that Gould column 5: lines 32-45 discloses transmitting the encrypted session packet to a biometric device. As mentioned previously, the Gould systems (figure 5) consists of three devices; a biometric device (292), a client (104), and a server (100). Gould column 5: lines 32-45 discloses the server (100) sending data to the client (104). Gould does not disclose an encrypted session packet or any other data being transmitted to the biometric device (292).

Second, the Examiner states that Gould figure 4: 420-426 discloses determining, based on a content of a collection of authentication information contained in the decrypted biometric information packet, whether or not to utilize a collection of biometric data contained in the decrypted biometric information packet. As mentioned under the claim 1 argument, the Gould process first determines whether or not to use the data (figure 4: 420) and then decrypts the data (figure 4: 422). Gould does not disclose making a determination after the data is decrypted as is recited in claim 35.

Claim 36:

On page 13 of the Office Action, the Examiner states that Michener (column 9: lines 5-40; Session-Random Number) discloses a method, wherein generating a session packet comprises generating a session number and storing it in the session packet. Applicant respectfully contends that Michener does not disclose this.

The cited section describes using the session random number to generate session keys and re-keying keys. The section does not disclose storing the session random number or any other number, in a session packet.

Claim 37:

On page 14 of the Office Action, the Examiner states that Michener (Column 10: lines 1-25; figure 13: Table Lookup: data structure) discloses a method, further comprising storing the session number in a database associated with the computing device. Applicant respectfully contends that Michener does not disclose this.

Michener figure 13 shows that the "Table Lookup" provides the "TADID_B" value. Michener column 8 line 26, states that this value is a TAD-specific 64 bit Binary ID. This number is not associated with a session, such as the session number recited in claim 37.

Claim 39:

On page 14 of the Office Action, the Examiner states that Michener (column 10: lines 1-15; figure 13: Table Lookup; data structure) discloses storing a session key in a database associated with the computer. Applicant respectfully contends that Michener does not disclose this.

The "Table Lookup" in Michener figure 13 provides the "TADID_B" value which is used to generate a session key. The session key itself is not stored in the "Table Lookup" or in any database associated with the computer.

Claim 43:

On page 15 of the Office Action, the Examiner states that Michener (figure 13) discloses a method, wherein generating a session packet comprises generating a session time stamp and storing it in the session packet. Applicant respectfully contends that Michener does not disclose this.

Michener figure 13 does not contain anything at all related to time. It certainly does not disclose generating or storing a session time stamp.

Claim 45:

On page 16 of the Office Action, the Examiner states that Michener (column 2: lines 15-60; figure 17) discloses a method wherein making a determination comprises evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period. Applicant respectfully contends that Michener does not disclose this.

The text of Michener column 2: lines 15-60 is listed immediately below.

> “various processing stages;
> FIG. 26a illustrates a structure of a TAD input command for loading a rekeying keyset;
> FIG. 26b illustrates a structure of a TAD response to a command for loading a rekeying keyset;
> FIG. 27a illustrates a structure of a TAD input command for installing a new working keyset;
> FIG. 27b illustrates a structure of a TAD response to a command for installing a new working keyset;
> FIG. 28a illustrates a structure of a TAD input command for installing a new language;
> FIG. 28b illustrates a structure of a TAD response to a command for installing a new language;
> FIG. 29a illustrates a structure of a TAD input command for identifying a TAD to a client computer;
> FIG. 29b illustrates a structure of a TAD response to a command for identifying a TAD to a client computer;
> FIG. 30a illustrates a structure of a TAD input command for testing a TAD maintenance key;
> FIG. 30b illustrates a structure of a TAD response to a command for testing a TAD maintenance key;
> FIG. 31a illustrates a structure of a TAD input command for personalizing a TAD; and
> FIG. 31b illustrates a structure of a TAD response to a personalizing a TAD.
> DESCRIPTION OF EMBODIMENT(S)
> Electronic communications, and the data which traverses those communications, are relatively new, as is the technology used to protect electronic data. Existing communications protection technologies tend to fall into two categories. The first, government sponsored, is generally very well thought out and provides excellent protection, but is not readily available for commercial applications. The second, de facto commercial, are mostly not strong enough to protect important information, or are dedicated to specific functions. For example, standard point-of-sale devices are dedicated to merchandizing applications, and existing ATM systems are dedicated to the dispensing of cash.
> There exists a need for a device to provide personal protection of electronic data that is small, easy to use, provides excellent protection to the PC/laptop user, and that can operate in conjunction with corresponding devices at a central data gathering point to provide near real time validation of the information.”

Applicant fails to see how Michener column 2: lines 15-60 (the language quoted above) could be viewed as disclosing evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period.

Similarly, applicant also fails to see how Michener figure 17 could possibly disclose claim 45. Michener figure 17 does not contain anything similar or related to evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period.

**Conclusion**

It is respectfully submitted that claims 1-3, 5, 10, 14, 23, 26-27, 29, 35-37, 39, 43, and 45 are patentably distinguishable from the Gould and Michener references, considered independently or in combination. It is also respectfully submitted that the dependent claims 4, 6-9, 11-13, 15-22, 24-25, 28, 30-34, 38, 42, 44, and 46-48, are patentable based on their dependence on patentable independent claims. Accordingly, reconsideration and allowance of all pending claims are respectfully solicited.

The Director is authorized to charge any fee deficiency required by this paper or credit any overpayment to Deposit Account No. 23-1123.

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.

By: Chris Holt
Christopher L. Holt, Reg. No. 45,844
900 Second Avenue South, Suite 1400
Minneapolis, Minnesota 55402-3319
Phone: (612) 334-3222 Fax: (612) 334-3312

CLH:rkp